Anti-Spam Gateway Product

DECISION PAPER – IT Security Assessment

Prepared by Cliff Schiller, IT Security Officer

IT Security Office — **Technical requirements for enterprise anti-Spam service**

Requirements:

The diverse nature of the department's business places extra challenges on the successful implementation of an anti-Spam service. A successful anti-Spam solution must have the flexibility for specific and broad-based exception processing. In several instances, incoming E-mail that would be considered Spam by some program areas is considered legitimate mail in others.

- General

The following general requirements exists for any vendor product or service:

1. Must be available for an in-house evaluation period of 30 to 60 days prior to the finalization of the purchase agreement.
2. Must operate as or at the SMTP gateway in front of the agency's E-mail service.
3. Vendor representative must provide on-site or immediate phone support during initial setup and configuration.

- Anti-Spam functions

In addition, the following system requirements must be considered to best meet the constantly changing and difficult demands for identifying incoming Spam or Unsolicited Commercial E-mail (UCE) within the Department of Health.

Anti-Spam software functions	**Desirable or Required**
Runs at SMTP Gateway (in front of the agency's E-mail servers)	Required
Supports Spam management (reporting, archiving)	Desirable
Incorporates use of a remote management console	Required
Supports automated vendor updates	Required
Configuration settings support use of groups	Desirable
Supports threshold limits	Desirable
Incorporates the following Spam handling options	
• Delete	Required
• Return to sender	Required
• Notify (sender and intended recipients)	Required
• Quarantine function – ☑ Per system ☑ Per group ☑ Per user	 Required Desirable Desirable
• Delay delivery	Desirable
• Spam forwarded to another addressee	Desirable
Supports multiple pass/multiple analysis techniques (See requirements for Spam analysis Techniques, Below)	Required

Prepared by Cliff Schiller, IT Security Officer

- Spam analysis techniques

Most anti-Spam services easily achieve a level of accuracy between 75% and 80% in identifying E-mail that is truly Spam. With the tremendous increase in volumes, the challenge for today's anti-Spam products is to do so within the smallest degree of error. Today, an error rate of 20% can produce quite a large number of Spam messages that make it into the agency's E-mail in-boxes. No single anti-Spam analysis technique can be 100 percent effective at stopping all spam. Two challenges exist

- False Positives – falsely identifying legitimate E-mail as Spam
- False Negatives – failure to identify real Spam as Spam

Anti-Spam solutions that have the lowest rate of false positives and false negatives incorporate multiple passes and multiple analysis techniques. The following are IT Security Office requirements for the analysis techniques used to identify Spam from legitimate mail.

Spam analysis Techniques	**Description – ability to identify and except/reject based on this criteria.**	**Desirable or Required**
DNS (Domain Naming Service) analysis	Assess whether E-mail comes from a valid host or Internet Service Provider	Required
Internet header analysis	Assess whether E-mail address is legitimate and has not been spoofed	Required
Statistical analysis	Assess one or more analysis components to statistically deduce the probability of E-mail as Spam	Required
Whitelisting	Assess against list of known good IP addresses	Required
Blacklisting	Assess against list of known bad IP addresses.	Desirable
Use of real-time black hole lists (RBL)	Same as blacklisting, list service provided by 3rd part vendor	Desirable
Open proxy lists	Similar to RBL, list service specific to identifying un protected E-mail relays that are open to spoofing	Desirable
Rate-limiting	Assess against the number of e-mails received from a single address per unit of time	Desirable
Message format analysis	Ability to assess multiple E-mail message formats including text, HTML, images, rich text, S/MIME	Required
HTML analysis	Ability to assess anomalies, randomly generated HTML tags, embedded URLs, graphics	Required
Analysis of attachments	Ability to assess popular attachment types including text, rich text, HTML, images, word processor documents, spread sheets, databases, etc.	Required